REMARKS

The § 103 Rejection

Claims 1-2 and 10 presently stand rejected under 35 U.S.C. § 103 as allegedly unpatentable over a combination including Raven et al (U.S. Patent No. 5,429,361) and Elliott et al (U.S. Patent No. 5,036,461). Without acquiescence in the grounds of the rejection, and without prejudice to pursue at a later time, Applicant has amended claim 1 to clarify the subject matter being claimed, and canceled claim 10. This rejection is thereby respectfully traversed.

In particular, claim 1 (as amended) is directed to a security device for use in a cashless system wherein portable data devices may be used to conduct cashless transactions, and includes, among other things, a "data device reader" adapted to receive and read portable data devices, a "host device physically proximate to said data device reader" and comprising a host device processor, and a "security module interposed between said data device reader and said host device processor and uniquely identified with said host device." Claim 1 has been amended to recite that the security module "prevent[s] completion of a transaction involving said data device reader and said host device processor unless said data device reader is successfully cross-authenticated with said security module when a portable data device is presented to and read by said data device reader, independent of any authentication of said portable data device by said data device reader." It is respectfully submitted that, by contrast, Raven et al 361 merely describes manual entry of a PIN to verify the user of a magnetic card (see, e.g., Raven et al '361 at col. 10, lns. 49-62), but does not teach or suggest cross-authentication of any type,

much less a cross-authentication between a "data device reader" and a "security module" that is "uniquely identified with said host device." Likewise, it is respectfully submitted that Elliott et al '461 fails to disclose or suggest the recited features. Elliot et al '461 describes an authentication procedure between a module and a smart card (see Elliot et al, Fig. 5 and col. 8, lns. 14 ff.), but neither discloses nor suggests a cross-authentication between a "data device reader" and a "security module" that is "uniquely identified with said host device." Thus, even if properly combinable, neither Raven et al '361 nor Elliott et al '461 disclose the features of claim 1, and Applicant respectfully submits that claim 1 should be allowable.

As previously noted, independent Claim 6 was not addressed in the Office Action, although it was not canceled in the Preliminary Amendment. Applicant respectfully submits that claim 6 is allowable over the cited items. Claim 6 is directed to a security module including a "data device reader interface for connection to a data device reader," a "gaming device interface for connection to a game device processor," and a "processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated." It is respectfully submitted that Raven et al '361 lacks, among other things, a "processor ... configured to prevent communication ... unless said data device reader is first authenticated." Rather, in Raven et al '361, the system attempts to verify the PIN entered by the user in connection with the user's magnetic card. There is no authentication of a "data device reader" as such. While Elliott et al '461 discusses

an authentication process between a module and a card, it does not teach or suggest a "processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated." By contrast, it is the smart card (i.e., "integrated circuit card") of Elliott et al '461 which authenticates a "terminal" (see col. 9, lns. 23-31), but Elliot et al '461 fails to teach or suggest use of a "processor" interposed between the data device reader interface and gaming device interface that is configured to prevent communication "unless said data reader device is first authenticated." Claim 6 thus provides a fundamentally different approach to security than attempted by Elliott et al '461, although the technique of claim 6 is not incompatible with additionally using authentication between a card and terminal or reader.

It is therefore respectfully submitted that claims 1 and 6 are allowable over the two cited patents. In addition, claim 2 depends from claim 1 and should be allowable for the same reasons as claim 1.

New Claims

New claims 11-22 have been added. Claims 11-15 and 16-17 depend from independent claims 1 and 6, respectively, which, as discussed above, should be in condition for allowance. Newly added claim 18 is an independent method generally analogous to claim 1, and new claims 19-22 depend therefrom. It is respectfully

submitted that claims 18-22 should be allowable for at least the same reasons as previously described for claim 1 above.

Request for Allowance

The undersigned has made a good faith effort to respond to all of the rejections in the case and to place the claims in condition for immediate allowance. Nevertheless, if any unresolved issue remains, the Examiner is invited to contact the undersigned by telephone to discuss those issues so that the Notice of Allowance can be mailed at the earliest possible date.

It is respectfully submitted that the instant application stands in condition for allowance, and a Notice of Allowance is earnestly solicited.

Respectfully submitted,

IRELL & MANELLA LLP

Dated: January 12, 2005

By: _____
Christopher A. Vanderlaan
Registration No. 37,747

1800 Avenue of the Stars, Suite 900
Los Angeles, California 90067-4276
(310) 277-1010

Customer No. 29000